AMA
AMERICAN MEDICAL ASSOCIATION

Checklist: Protecting office computers in medical practices against cyberattacks

Viruses, malware and hackers pose a threat to patient information and to your medical practice. Follow these tips to keep your office computers safe.

Accounts and passwords

- Do not share log-in information with anyone inside or outside of the organization.
- Make sure each staff member has a unique user account name and password.
- Create and enforce a strong password policy. Use at least eight characters with a combination of letters, numbers and symbols. Change the password every 90 days at a minimum. Lock the computer (e.g., Windows key + L) when it is not in use and require a password anytime a locked/screensaver-enabled computer is accessed.

Administrative accounts and software installs

- Most users in an organization do not need to be authorized as system administrators with expanded system access and capabilities.
- Create a Limited User Account for everyday use and keep the Administrator access for special tasks (e.g., software installation).
- Audit software applications on each computer, maintaining a list of approved software applications and removing any unauthorized software as soon as it is detected.
- Consider an application "whitelisting" strategy. A whitelisting strategy is one in which only safe, authorized and necessary applications can execute and run on computer systems or networks.

Operating system updates (also known as "patches")

- Check the computer's settings to ensure the system will automatically download and install new versions of operating system and Microsoft Office software.
- Note when the computer will install these new updates and make sure the computer is on at that time.

Web browser software updates

Make sure to use the most current version of the web browser software (e.g., Internet Explorer, Chrome and Firefox) and enable automatic updates if possible.

Anti-virus software

- Purchase and install anti-virus software.
- Since anti-virus software needs Internet access to download the most current virus profiles, ensure that the computer has regular access to the internet.
- It may be most convenient to set the update times for after business hours.
- Make sure to leave the computer on when the software is set to update.
- Make sure updates occur at least once a week.

Macros

Microsoft Office applications use macros to automate routine tasks. However, macros can contain malicious code that can be used to exploit vulnerable systems. As a precaution and unless otherwise needed, make sure macros are disabled in Office.

The process to disable macros is different depending on the version of Office, however, it is typically found under the "Options" setting in the "File" menu. Also note that macros may need to be disabled for each program in Office—including Word and Excel.

Additional computer software

Many office computers run additional software that supports everyday work. While one may not directly notice this software running on the computer, it is very important that these applications are updated and running the most current versions (e.g., Adobe Reader and Adobe Flash).

Firewalls: Mac operating systems

To find what version of Mac OS is running, click on the Apple icon in the top left corner of the screen. From there, click "About this Mac." A window should appear in the middle of the screen with information about the OS.

Mac OS X v10.5

- Choose "System Preferences" from the Apple menu.
- Click "Security."
- Click the "Firewall" tab.
- Choose which mode you would like the firewall to use.

Mac OS X v10.6 and later

- Choose "System Preferences" from the Apple menu.
- Click "Security" or "Security & Privacy."
- Click the "Firewall" tab.
- Unlock the pane by clicking the lock in the lower-left corner and enter the administrator username and password.
- Click "Turn on Firewall" or "Start" to enable the firewall.
- Click "Advanced" to customize the firewall configuration.

Firewalls: Windows operating systems

To find what version of Windows is running, click the "Start" button, type "computer" in the search box and hit "Enter." Right-click on "Computer" and then click "Properties" or "System Properties." Look under Windows edition for the version and edition of Windows that is running.

Windows 7

- Open Windows Firewall by clicking the "Start" button and then clicking "Control Panel." In the search box, type "firewall," and then click "Windows Firewall."
- In the left pane, click "Turn Windows Firewall on or off." If prompted for an administrator password or confirmation, type the password or provide confirmation.
- Click "Turn on Windows Firewall" under each network location to be protected and then click "OK."
- Note: Windows 7 is no longer supported by Microsoft unless you pay for extended support. Microsoft is offering a paid **extended security update** service for Windows 7 until January 2023.

Windows 10

- In search box, type "firewall" and then select "Windows Firewall."
- Select "Turn Windows Firewall on or off." If prompted, enter an administrator password or confirm.

This is intended to provide a jumpstart in improving physician practice cybersecurity but should not be considered exhaustive.

20-444373:PDF:4/20